ITRI 625

Pfleeger Chapter 11

Legal and ethical issues in computer security

- There are three motivations for studying the legal aspects of computer security:

1. To know what protection the law provides for computers and data.

2. To appreciate laws that protect the rights of others with respect to computers, programs and data.

3. To understand existing laws as a basis for recommending new laws to protect computers, data, and people.

We need to protect computing systems against criminals, code and data, programmers' and employers' rights, and users of programs.

Protecting programs and data

- Copyrights. First step is notice, then filing at the copyrights office.
- Intellectual property.
- Originality of work.
- Fair use of material.
- Copyrights for digital objects. The Digital Millennium Copyright Act (or DMCA) came into effect in 1998.
- Patents. Obtained by convincing the patent office that an invention deserves a patent. Not encouraged for computer software.

Protecting programs and data *cont.*

- Trade secrets. Information that gives one company a competitive edge over others.
- Can be discovered through reverse engineering. Start with the finished product and work backwards.
- Extremely applicable to computer objects as it allows distribution of the result of a secret while still keeping the program design hidden.
- See table 11.1 on page 716 for a summary.

Rights of employees and employers

- The age old question of who owns a product?
- Patent ownership is based on who files the patent application.
- In general with copyrights the creator is considered to be the owner of the work.
- In a work for hire situation the employer is considered the author of a work. The employer is seen as coming up with the idea.
- Licenses. With licenses the programmer is considered the author, which then provides license for companies to use the work.
- Employment contracts often spell out rights of ownership.

Computer crime

- Rules of property. The legal system has explicit rules about what constitutes property.
- Rules of evidence. The biggest difficulty with computer based evidence in court is being able to demonstrate the authenticity of the evidence.
- Threats to integrity and confidentiality. The integrity and secrecy of data are also issues in many court cases.
- Value of data. How much is data that has been stolen really worth?
- Acceptance of computer terminology. The law is lagging behind technology in its acceptance of definitions of computing

  terms.

Computer crime *cont.*

- Computer crime is hard to prosecute for the following reasons:

1. Lack of understanding.
2. Lack of physical evidence.
3. Lack of recognition of assets.
4. Lack of political impact.
5. Complexity of case.
6. Age of defendant.

Ethical issues in computer security

- It is impossible or impractical to develop laws to describe and enforce all forms of behavior acceptable to society. Society tends to rely on ethics to prescribe generally accepted standards of proper behavior.

- An ethic is an objectively defined standard of right and wrong. A set of ethical principles is called an ethical system.

- See table 11.3 on page 745 for a contrast of law vs. ethics.

- Ethics and religion. Although they might influence one another, the one does not determine the other.
- Ethical principles are not universal. Ethical values vary by society, and from person to person within a society.

Ethical issues in computer security *cont.*

- Ethics does not provide answers. Ethical pluralism is recognizing or admitting that more than one position may be ethically justifiable in a given situation.
- See table 11.4 on page 750 for a taxonomy of ethical theories.
- Also see section 11.7 for case studies of ethics.
- Because of such ethical issues, various computer groups have sought to develop codes of ethics for their members. Among these are the IEEE, ACM, and the computer ethics institute.

Questions

- Any Questions?